



Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DOD-2016-OS-0092]

Privacy Act of 1974; System of Records

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Notice to add a System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974, 5 U.S.C. 552a, and Office of Management and Budget (OMB) Circular No. A-130, notice is hereby given that the Office of the Secretary of Defense proposes to add a new system of records, DSCA 07, entitled "Security Assistance Network (SAN)." The SAN is the international security cooperation (SC) database and communications network that provides the Security Cooperation Offices (SCOs) and others in the SC community access to SC financial and logistics management systems, information via various bulletin boards, and a library system for large files. The SAN provides the primary interface for the input and output of data from all military departments, SCOs, and International Military Student Offices (IMSOs). Most importantly, the SAN is where the SCO training manager obtains data used for the Security Cooperation Training Management System (SC-TMS). All SCOs and IMSOs must use the SAN and its components to perform their assigned SC training management functions.

DATES: Comments will be accepted on or before [**INSERT 30-DAYS FROM DATE OF PUBLICATION IN THE FEDERAL REGISTER**]. This proposed action will be effective the day following the end of the comment

period unless comments are received which result in a contrary determination.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

- * Federal Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.

- * Mail: Department of Defense, Office of the Deputy Chief Management Officer, Directorate of Oversight and Compliance, 4800 Mark Center Drive, Mailbox #24, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <http://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Mrs. Luz D. Ortiz, Chief, Records, Privacy and Declassification Division (RPD2), 1155 Defense Pentagon, Washington, D.C. 20301-1155, or by phone at (571) 372-0478.

SUPPLEMENTARY INFORMATION: The Office of the Secretary of Defense notices for systems of records subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended, have been published in the Federal Register and are available from the address in **FOR FURTHER INFORMATION CONTACT** or at the Defense Privacy, Civil Liberties, and Transparency Division website <http://dpclld.defense.gov/>.

The proposed system report, as required by 5 U.S.C. 552a(r) of the Privacy Act of 1974, as amended, was submitted on September 2, 2016, to the House Committee on Oversight and Government Reform, the Senate Committee on Governmental Affairs, and the Office of Management and Budget (OMB) pursuant to paragraph 4c of Appendix I to OMB Circular No. A-130, "Federal Agency Responsibilities for Maintaining Records About Individuals," revised November 28, 2000 (December 12, 2000 65 FR 77677).

Dated: September 16, 2016.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

DSCA 07

System name:

Security Assistance Network (SAN)

System location:

Institute for Defense Analysis (IDA), 4850 Mark Center Drive, Alexandria, VA 22311-1882.

Categories of individuals covered by the system:

DoD civilian, military, contractor personnel (collectively, "U.S. personnel"), and individuals with dual citizenship with the U.S., selected to attend DoD security cooperation training (collectively, "students").

Categories of records in the system:

Security Cooperation Training Management System (SC-TMS):

U.S. Personnel Data: Name, organization, office telephone and fax numbers, point of contact function, and military rank.

Student Data: Full name and alias, full face photograph, gender, citizenship, nationality, date and place of birth, physical descriptions, e-mail addresses, work and home addresses, work and home telephone numbers, marital status, military rank and date of rank, branch of military service, worksheet and student control numbers, clearance, passport and visa information, health information, lodging and travel information, emergency contact(s), language capabilities, educational and employment information, academic evaluation, religious affiliation, personal preferences (i.e., dietary needs, religious accommodations, customs and traditions), activity remarks, and dependency data (if accompanied).

Security Cooperation Workforce Database (SCWD):

U.S. Personnel Data: Name, DoD Identification Number (DoD ID Number), military rank, position number, source and title, funding source, billet category, headquarters, current service, organization, country, state, rotate date, minimal training, and level of training.

International Affairs Certification Database (IACD):

U.S. Personnel Data: Full name, personal or work email address, mailing address, telephone and fax number, major command and work mailing address, name of organization, office symbol/code, job title, job function, grade/rank, job series, military specialty, start date, total months in International Affairs related work, billet information, current certification level, highest education completed, and field of study. Supervisor information that consists of the first and last name, work email address, organization, office symbol, work phone, and fax number.

Authority for maintenance of the system:

10 U.S.C. 134, Under Secretary of Defense for Policy; 22 U.S.C. 39, Arms Export Control Act, Chapters 32 and Chapter 39; DoD Directive (DoDD) 5105.65, Defense Security Cooperation Agency (DSCA); DoDD 5101.1, DoD Executive Agent; DoDD 5132.03, DoD Policy and Responsibilities Relating to Security Cooperation; Army Regulation 12-15, Secretary of the Navy Instruction 4950.4B/Air Force Instruction 16-105, Joint Security Cooperation Education and Training; and DSCA Manual 5105.38-M, Security Assistance Management Manual (SAMM), Chapter 10, International Training.

Purpose(s):

The SAN is a network used to exchange Security Cooperation personnel management, training, and budget information between overseas Security Cooperation Offices, Geographical Combatant Commands, Military Departments, Defense Security Cooperation

Agency (DSCA), Defense Finance and Accounting Services (DFAS), DoD Schoolhouses, Regional Centers, and international host nation organizations.

The SAN hosts the Security Cooperation Training Management System (SC-TMS) which are tools used by the Security Cooperation community to manage student training data, including the Security Cooperation Workforce Database (SCWD) and International Affairs Certification Database (IACD) which tracks and provides the status of training for the Security Cooperation workforce certification levels.

In addition, the SAN hosts the Security Assistance Automated Resource Management Suite and the Security Cooperation International Resource Management System, both of which are budget programs that do not collect personally identifiable information (PII).

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows to:

Law Enforcement Routine Use: If a system of records maintained by a DoD Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

Congressional Inquiries Disclosure Routine Use: Disclosure from a system of records maintained by a DoD Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

Disclosures Required by International Agreements Routine Use: A record from a system of records maintained by a DoD Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

Disclosure to the Department of Justice for Litigation Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

Disclosure of Information to the National Archives and Records Administration Routine Use: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to the National Archives and Records Administration for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

Data Breach Remediation Purposes Routine Use: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies,

entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:

Storage:

Paper records and electronic storage media.

Retrievability:

Individual's name, DoD Identification Number, Worksheet Control Number, or Student Control Number.

Safeguards:

Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, and is accessible only to authorized personnel. Access to records is limited to person(s) responsible for servicing the record in performance of their official duties and who are properly screened and cleared for need-to-know. Access to computerized data is restricted by centralized access control to include the use of CAC, passwords, file permissions, and audit logs.

Retention and disposal:

Destroy five years after completion of a specific training

program, after period covered by account, from last activity or when superseded or obsolete, whichever is sooner.

System manager(s) and address:

SAN System Administrator, Defense Institute of Security Management, 2475 K. Street, Bldg. 52, Wright-Patterson AFB, OH 45433-7641.

Notification procedure:

Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to Defense Institute of Security Management, ATTN: Director of International Studies or Director of Research, 2475 K Street, Wright-Patterson AFB, OH 45433-7641.

Signed, written requests should include the full name, DoD ID Number (if applicable), current address and telephone number, and the name and number of this system of records notice.

In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

Record access procedures:

Individuals seeking access to records about themselves contained in this system should address written inquiries to the Office of the Secretary of Defense/Joint Staff, Freedom of Information Act Requester Services, 1155 Defense Pentagon, Washington, DC 20301-1155.

Signed, written requests should include the full name, DoD ID number (if applicable), current address and telephone number, and the name and number of this system of records notice.

In addition, the requester must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories,

possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

Contesting record procedures:

The OSD rules for accessing records, for contesting contents and appealing initial agency determinations are published in OSD Administrative Instruction 81; 32 CFR Part 311; or may be obtained from the system manager.

Record source categories:

Individual or service organization.

Exemptions claimed for the system:

None.

[FR Doc. 2016-22807 Filed: 9/21/2016 8:45 am; Publication Date: 9/22/2016]